Tipos de atacantes

Codificación	Definición
Hackers	Expertos informáticos con una gran curiosidad por descubrir las vulnerabilidades de los sistemas pero sin motivación económica o dañina.
Crackers	Un hackers que, cuando rompe la seguridad de un sistema, lo hace con intención maliciosa, bien para dañarlo o para obtener un beneficio económico.
Phreakers	Crackers telefónicos, que sabotean las redes de telefonía para conseguir llamadas gratuitas.
Sniffers	Expertos en redes que analizan el tráfico para obtener información extrayéndola de los paquetes que se transmiten por la red.
Lammers	Chicos jóvenes sin grandes conocimientos en informática pero que se consideran a sí mismos hackers y se vanaglorian de ellos.
Newbie	Hacker novato.
Ciber terrorista	Expertos en informática e intrusiones en la red que trabajan para países y organizaciones como espías y saboteadores informáticos.
Programadores de virus	Expertos en programación, redes y sistemas que crean programas dañinos que producen efectos no deseados en los sistemas o aplicaciones.
Carders	Personas que se dedican al ataque de los sistemas de tarjetas, como los cajeros automáticos.

Técnicas de ataque

- **Malware**: es un término general para referirse a cualquier tipo de software malicioso diseñado para infiltrarse en su dispositivo sin su conocimiento y causar daños e interrupciones en el sistema o robar datos.
    - Virus: son programas informáticos que tienen como objetivo alterar el funcionamiento del computador, sin que el usuario se de cuenta.
    - Troyano: oculta software malicioso dentro de un archivo que parece normal.
    - Gusano: son en realidad una subclase de virus, por lo que comparten características. Son programas que realizan copias de sí mismos, alojándolas en diferentes ubicaciones del ordenador.
    - Puerta trasera: se denomina a cualquier punto débil de un programa o sistema mediante el cual una persona no autorizada puede acceder a un sistema.
    - Programas conejo: es aquel cuya principal función, como si de un conejo se tratase, es la de reproducirse infinitamente, copiándose a sí mismo consumiendo los recursos del sistema informático atacado.
    - Spyware: es un software maliciosos diseñado para espiar su actividad en Internet y recopilar datos personales sin su conocimiento o consentimiento
    - Adware: es un tipo de programa publicitario malicioso.
    - Ransomware: es un tipo de malware o código malicioso que impide la utilización de los equipos o sistemas que infecta.

- **Spoofing**: consiste en usurpar una identidad electrónica para ocultar la propia identidad y así cometer delitos en Internet.

- **Sniffing**: es un software o hardware que se utiliza para monitorizar, capturar y analizar en tiempo real los paquetes de datos que pasan por una red, sin redirigirlos ni alterarlos.

- **Keylogger**: son tecnologías utilizadas para controlar y rastrear las pulsaciones de cada tecla en los dispositivos electrónicos, ya sea un teclado físico, un ratón o una pantalla.

- **Denegación de servicio (DDoS)**: es un tipo de ciberataque que intenta hacer que un sitio web o recurso de red no esté disponible colapsándolo con tráfico malintencionado para que no pueda funcionar correctamente.

- **Ingeniería social**: es una técnica que emplean los ciberdelincuentes para ganarse la confianza del usuario y conseguir así que haga algo bajo su manipulación y engaño.

    - Phishing: es un tipo de estafa digital que consiste en robar, mediante engaños, información confidencial de las personas, como contraseñas o números de tarjetas de crédito.

    - Spam: los mensajes Spam en formato HTML pueden, por ejemplo, contener scripts potencialmente peligrosos.

- **Pharming**: es muy semejante al phishing, en el que el tráfico de un sitio web es manipulado para permitir el robo de información confidencial.

- **Password cracking**: es el proceso de recuperación de contraseñas que se han almacenado en un equipo.

- **Botnet**: es un conjunto de ordenadores, denominados bots, infectados con un tipo de malware que son controlados remotamente por un atacante y que pueden ser utilizados de manera conjunta para realizar actividades maliciosas.

Noticias sobre DDoS, Phishing y Ramsonware:

DDoS:
https://elpais.com/tecnologia/2009/12/24/actualidad/1261648862_850215.html

https://computerhoy.com/noticias/tecnologia/ataque-ddos-grande-historia-fue-semana-pasada-superando-20-anterior-1102539

Phishing:
https://www.eldiario.es/castilla-la-mancha/universidades/universidad-castilla-mancha-advierte-campana-phising-correos-electronicos_1_10548656.html

https://www.20minutos.es/tecnologia/netflix-ciberseguridad-aviso-incibe-tu-suscripcion-netflix-no-ha-caducado-se-trata-un-phishing-5162001/

Ransomware:
https://www.20minutos.es/tecnologia/ciberseguridad/posible-ciberataque-sony-afirman-acceso-todos-sistemas-compania-incluidos-datos-playstation-5176229/

https://www.xataka.com/seguridad/ciberataque-paraliza-ayuntamiento-sevilla-piden-rescate-cinco-millones-euros-para-recuperarlo